

ATTACHMENT C

AFFIDAVIT OF JOHN CHEVALIER

I, John Chevalier, Task Force Officer of the Federal Bureau of Investigation, Memphis Division, being duly sworn, state that the following information is true and correct to the best of my knowledge, information and belief:

1. I am a Memphis Police Officer and have been so employed since August 10, 1998. I have also been sworn as a Special Federal Officer and a Special Deputy United States Marshal. I am currently assigned full-time to the FBI's Memphis Child Exploitation Task Force. Throughout my law enforcement career I have arrested countless individuals for violations of law, both misdemeanor and felonious in nature. I have also participated in multiple search warrants leading to the seizure of items having evidentiary value; these seizures have aided in the successful arrest and prosecution of individuals involved in criminal activity. Since joining the Task Force I have received training on the investigation and prosecution of child exploitation cases and I have experience in Sex Crimes investigations. I have gained experience through training in seminars, classes and everyday work related to conducting these types of investigations.

2. As a FBI Task Force Officer, your Affiant is authorized to investigate crimes involving the sexual exploitation of children pursuant to Title 18, United States Code, Section 2252(a) makes it a federal offense to knowingly possess, access, transport, receive, or distribute a visual depiction, the production of which involving the use of a minor engaging in sexually explicit conduct, if such visual depiction is of such conduct, or to attempt to do so, if that visual depiction has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, or the visual depiction was produced using materials that have been so mailed, shipped or transported. "Sexually explicit conduct" is defined in 18 U.S.C. § 2256(2)(A), and includes sexual intercourse of any kind, whether between persons of the same or opposite sex; bestiality; masturbation; and the lascivious exhibition of the genital or pubic area

3. Your Affiant has conducted and/or participated in investigations relating to the sexual exploitation of children. During these investigations I have observed and reviewed examples of child pornography in various forms of media including computer media. Your Affiant has received training and instruction in the field of investigation of child pornography, child sexual exploitation, and human trafficking and in the area of forensic extraction of digital evidence.

4. This application is part of an investigation into Keith Runyon (hereinafter RUNYON) for the alleged knowing possession of visual depictions of minors engaging in sexually explicit conduct (hereinafter, "child pornography").

5. The following information was obtained through observations and conversations of your Affiant personally, through the assistance of other law enforcement agents and agencies, including their reports, and through other sources specifically named in this affidavit. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violation of Title 18 U.S.C. §§ 2251 and 2252 will be located on the device described in **Attachment A**, and consist of or be contained in the items listed in **Attachment B**, which are incorporated by reference as if fully set forth herein.

PROBABLE CAUSE

6. On October 31, 2022 the United States Probation Office (USPO) for the Western District of Tennessee conducted a status check of RUNYON at the Memphis Union Mission (MUM), 383 Poplar Avenue in Memphis, Shelby County, Tennessee. The Memphis Union Mission ministers to the physical, spiritual and emotional needs of men, women, and families who are homeless, addicted and in crisis. RUNYON is a registered sex offender in the State of Tennessee and is under Community Supervision for Life by the Tennessee USPO. RUNYON signed a Community Supervision Certificate acknowledging this supervision which includes a warrantless search of his person, vehicle, property or place of residence at any time by a probation officer. During this status check, Probation Officer Michael Alston (ALSTON) of USPO collected RUNYON's Motorola Moto G Pure cellular telephone. RUNYON told

ALSTON that he was given the phone by another homeless individual at the MUM in either June of July 2022 and that he used the phone to view pornographic images daily.

7. ALSTON sent the Motorola Moto G Pure cellular telephone to Forensic Examiner Zachary Hailey (HAILEY) in the Eastern District of Missouri. Following an examination of the cellular telephone by HAILEY, a report was provided to Alston. Images depicting child pornography were found during the review of the phone. HAILEY's report listed three images found during his review, the following was taken from his report: The first image, named "2de07d2beef8713a_0," depicts a minor female performing oral sex on a nude minor male. The URL <http://xxxabclove.ru/2b708611f3cff8424e1b59a6b9bb5d3d/thumbs/79.jpg> is located inside the cached file. This site was last visited on October 2, 2022. The second image, named "73df4458898677d9_0," depicts a minor of unknown gender performing oral sex on an adult penis. The minor appears to be nude, and the genitals of the minor cannot be seen. The URL <http://amonga.fun/cac/22.jpg> is located inside the cache file. This site was last visited on October 2, 2022. The EXIF data of the image shows it was captured with a Sony cyber shot (Model: DSC-S60) on June 16, 2007. The third image, named "83ab773399d0c388_0," depicts a naked prepubescent minor being vaginally penetrated by an adult penis. The URL <http://amonga.fun/cac/02.jpg> is associated with the image. This site was last visited on October 2, 2022.

8. On 3-15-2023, USPO Evidence Custodian Freddie McMaster provided your Affiant with the Motorola Moto G Pure cellular telephone belonging to RUNYON as well as the forensic extraction of the phone performed by HAILEY. Both are now housed at the FBI Memphis field office.

BACKGROUND ON CHILD EXPLOITATION MATERIAL



9. Your Affiant, through training and experience, is aware that individuals who have an interest in possessing and sharing child pornography frequently maintain collections of images they have obtained, often for time periods of several years and longer. Digital storage devices have become mobile and physically smaller while increasing in storage capacity, thus making it easy for collectors to conceal their interest in child exploitation from friends, co-workers, and family members. In addition, the declining cost of digital storage devices and the availability of remote (“cloud”) storage can facilitate the maintenance of ever larger collections. Your Affiant is also aware, through training and experience, that digital storage devices have become interconnected, making it easy for even casual users of technology to transfer or copy images from one device to another, or to maintain duplicate copies on more than one device or storage medium. In fact, many devices such as smartphones can be set to automatically back up their contents to alternate storage facilities, such as laptop or desktop computers, another phone, photo-sharing websites, and cloud storage providers.

10. Your Affiant is aware that the contents of smart phones can be synched with or backed up to other digital devices in a variety of ways. Smartphones can be connected through cables to other devices, such as laptop computers, for data transfer. Smartphones can also connect to other devices and transfer photos or documents wirelessly through technology such as Bluetooth. Data can also be sent from the phone to an email account via the Internet, and subsequently downloaded from the Internet to a different device (such as a tablet, game system, or computer) for storage. In addition, many smartphones utilize “cloud” storage. Cellular telephones can be set to automatically back up their contents to user accounts hosted on servers of various cloud storage providers. Users can also opt to perform a back-up manually, on an as-needed basis. Your Affiant is aware that some smartphones also back up their contents automatically to devices such as laptop computers. Additionally, cellular telephones can exchange data between two differing cellular communications devices and other types of electronic and media storage devices via Bluetooth or Wi-Fi, regardless of the type of operating system or platform being utilized to operate each of the electronic devices. In addition, media cards which contain many forms of data can be interchanged between multiple types of electronic devices, including but not limited to, different cellular telephones.

11. Your Affiant has participated in the execution of numerous search warrants involving digital storage media evidence, to include cellular telephones. Your Affiant has discovered evidence, to include digital storage media and laptop computers, in the personal vehicles used by subjects for travel between their residences and places of business. Furthermore, your Affiant has knowledge that users of smartphones generally keep the phones on or near their person for convenience and ease of access.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

12. As is the case with most digital technology, communications by way of computer and cell phone can be saved or stored on the device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., in temporary files or within Internet service provider (ISP) client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

13. The search procedure for electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;
- b. on-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene

until that imaging can be completed;

- c. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- d. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- e. surveying various file directories and the individual files they contain;
- f. opening files in order to determine their contents;
- g. scanning storage areas;
- h. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment B**; and
- i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment B**.

14. Your Affiant is aware, through previous investigations, computers and cell phones are, in part or whole, manufactured outside the state of Tennessee.

15. In consideration of the foregoing, your Affiant respectfully requests that this Court issue a search warrant for the Motorola Moto G Pure cellular telephone cell phone belonging to Keith Runyon and the forensic extraction performed by Zachary Hailey, currently in the control and possession of the Federal Bureau of Investigation Memphis Field Office, more specifically described in **Attachment A**,



which is incorporated by reference as if fully set forth herein authorizing the seizure and search of the items described in **Attachment B**.

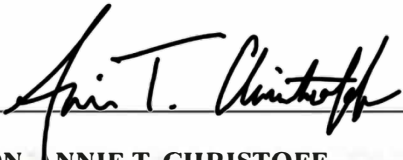
AND FURTHER, AFFIANT SAITH NOT.



JOHN CHEVALIER - AFFIANT

Task Force Officer, Federal Bureau of Investigation

Sworn to and subscribed before me on this 21st day of March, 2023.



HON. ANNIE T. CHRISTOFF
UNITED STATES MAGISTRATE JUDGE